C L A I M S

1. Method for authenticating a third tier server system in a distributed application environment, wherein said distributed application environment comprising client system having parts of the distributed application, server systems having the remaining parts of the distributed application (server application or server components), and third tier server system which exchanges data between said client system and said server systems, wherein said client system acts as single point of recognizing and managing third tier server certificates and provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment, wherein at said server systems side said method comprises the steps of:

receiving from said common database of said client system all necessary information of said third tier server certificate being accepted as trustworthy for determining to accept or to decline a connection to said third tier server,

comparing said information received from said client system with a third tier certificate received from said third tier server system,

accepting said third tier server system as to be authenticated if said information from said client system and said third tier certificate matches.

2. Method according to claim 1, wherein said information from said client system is received via a non-continuous client-server connection.

3. Method according to claim 2, wherein said non-continuous client- server connection is using a secure transmission protocol.

4. Method according to claim 1, wherein said necessary information of said third tier server certificate consist of an original third tier server certificate as stored in the common data base of said distributed application environment, and a server name which has transmitted said original third tier server certificate to said client system.

5. Method according to claim 1, wherein said necessary information of said third tier server certificate consist of a fingerprint of the original third tier certificate, and a server name which has transmitted said third tier server certificate to said client system.

6. Method according to claim 1, wherein said necessary information of said third tier server certificate consists of two different fingerprints of the original third tier server certificate, a server name which has transmitted said third original tier server certificate to said client system, and a certificate name.

7. Method for authenticating a third tier server system in a distributed application environment, wherein said distributed application environment comprising a client system having parts of the distributed application, server systems having the remaining parts of the distributed application (server application or server components), and a third tier server

system which exchanges data between said client system and said server systems, wherein said client system provides access to a common data base of the distributed application environment which contains third tier server certificates received from said third tier server which have been accepted as trustworthy for the distributed application environment, wherein at said client system said method comprises the steps of:

receiving a third tier server certificate from a third tier server system,

determining whether said received third tier server certificate can be accepted as trustworthy,

storing said third tier server certificate in said common data base of the distributed application environment if said third tier server certificate has been accepted as trustworthy,

transferring to each server of said server systems all necessary information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server system.

8. Method according to claim 7, wherein said storing step additionally includes name of said third tier server system that has transmitted said third tier certificate.

9. Method according to claim 7, wherein said third tier server certificate is received via a secure transmission protocol.

10. Method according to claim 7, wherein said necessary information of said third tier server certificate is transmitted to said each server of said server systems via a non-continuous secure connection.

11. Method according to claim 8, wherein authentication of said client system is accomplished by user ID and/or password.

12. Server systems (2) for authenticating third tier server system (3) in a distributed application environment, wherein said distributed application environment comprises a client system (1) having parts of the distributed application, a connection negotiator component (60) for receiving incoming third tier server certificates via a secure connection from said third tier server (3), a common data base (4) of the distributed application environment which contains third tier server certificates received from said third tier server (3) which have been accepted as trustworthy for the distributed application environment, a Certificate verifier component (50) for comparing received third tier server certificate with information stored in said common database and storing them into said common database if it matches, an user interface component(40) allowing to reject or accept an unknown third tier server certificate not contained in said common data store, a certificate transmitter component (30) for extracting all necessary information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database and transmitting them to said server systems (2) via a secure connection (a), and server systems (2) having the remaining parts of the distributed application (server application or server components), and said third tier server system (3) which exchanges data between said client system (1)

and said server systems (2), wherein each server of said server systems comprising:

transfer server component (120) which supports non-continuous and secure client-server connection for receiving all necessary information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a connection to said third tier server system (3),

a connection negotiator component (140) for receiving incoming third tier server certificate via a secure connection between said server systems and said third tier server,

a certificate verifier component (130) for comparing said third tier server certificate with said received necessary information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server.

13. System according to claim 12, wherein said necessary information of said third tier server certificate comprises two different fingerprints of the original third tier server certificate, name of the server which has transmitted said third tier server certificate to said client system, and certificate name.

14. System according to claim 13, wherein said different fingerprints are generated by applying two different algorithms to said third tier server certificates received from said common database.

15. System according to claim 14, wherein said server systems further include the same algorithms as used for generating said two different fingerprints.

16. Client system (1) for authenticating third tier server (3) in a distributed application environment, said distributed application environment comprises a client system (1) having parts of the distributed application, server systems (2) having the remaining parts of the distributed application (server application or server components) as well as a transfer server component (120) supporting non-continuous and secure client-server connection, a connection negotiator component (140) for receiving incoming third tier server certificate via a secure connection between said server systems (2) and said third tier server (3), a certificate verifier component for comparing said third tier server certificate received from said third tier server with said information received from said client system for determining to accept or to reject third tier server, and a third tier server which exchanges data between said client system and said server systems, said client system (1) comprising:

a connection negotiator component (60) for receiving incoming third tier server certificate via a secure connection from said third tier server (3),

a common data base (4) of the distributed application environment which contains third tier server certificates received from said third tier server system (3) which have been accepted as trustworthy for the distributed application environment,

a Certificate verifier component (50) for comparing received third tier server certificate with information stored in said common database (4) and storing them into said common database if it matches,

a user interface component (40) allowing to reject or accept an unknown third tier server certificate not contained in said common data store,

a certificate transmitter component (30) for extracting all necessary information of said third tier server certificates being accepted as trustworthy for determining to accept or to decline a third tier server from said common database and transmitting them to said server systems via a secure connection.

17. Computer program product stored in the internal memory of a digital computer, containing parts of software code to execute the method in accordance with claim 1-11 if the product is run on the computer.